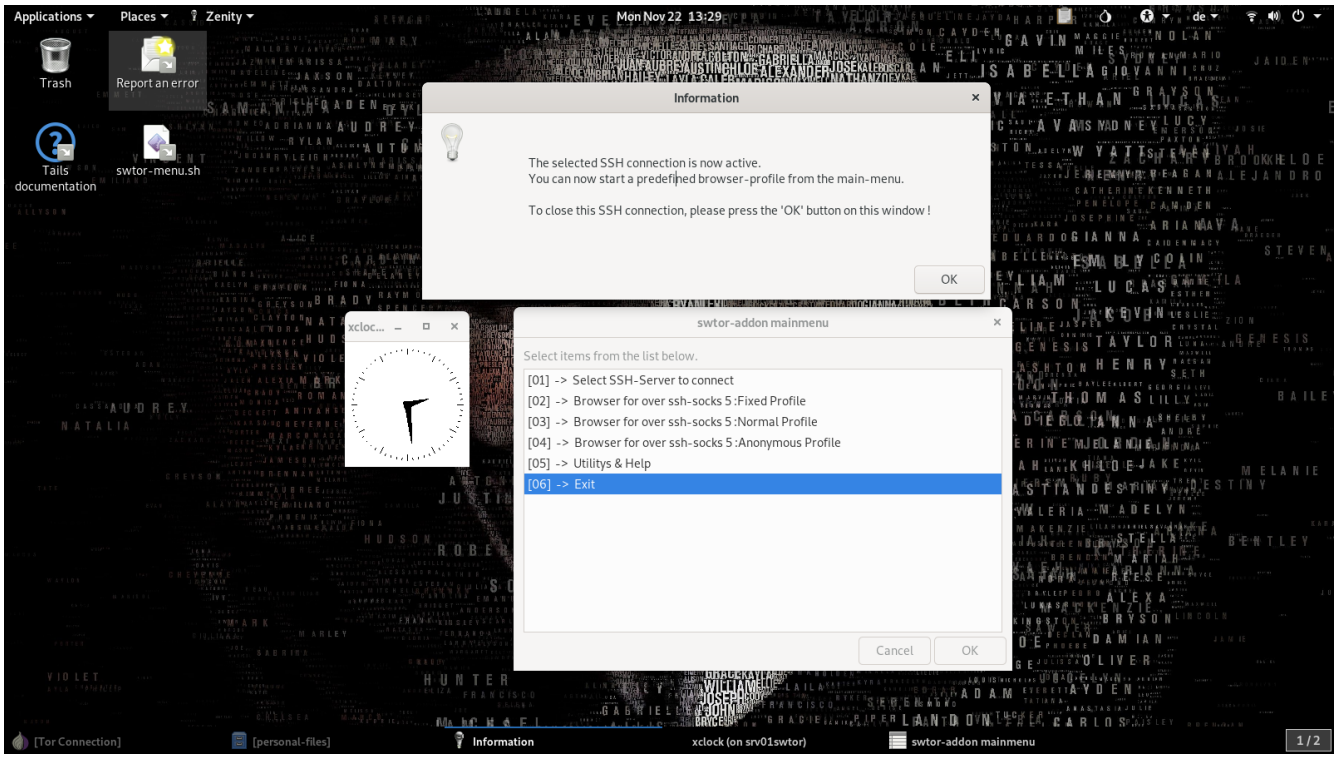
Documentation for the add-on to Tails

Author	:	swtor00@protonmail.com
Date	:	31.12.2021
Version	:	Release 0.60
Licence	:	GPL 2.0



In the year 2017 I began to write the first implementation of this script for my personal use only. This first implementation was a very huge shell script and was running with Tails 2.2 in the background. My first attempt for this script was not for browsing Tor unfriendly Sites. I was using Tails almost everyday and as soon I received a call from a customer I had to shutdown Tails and boot my Windows System where all the Customer VPN's are stored. At the end I was tired of rebooting every half hour to work only for a couple of minutes and then reboot again with Tails. With the working SSH-connection I was able to help my Customers (over VNC-Viewer or rdesktop for Linux) even If I was directly inside of a Tails session. At this point I began to realize that this ugly first script also could be used to visit multiple Websites without blocked services or even "captcha terror" because I was using Tails.

This first shell-code script was growing fast and ended in a little mess to extend and maintain as well. And, yes ... it was ugly to use and not very well integrated into Tails. Prior to version 3.8 of Tails, it wasn't possible to install software over the GUI. It was possible for me to implement this feature on the terminal only. My first script was only a terminal based shell script presented without any fancy GUI. The source-code was not openly available to the public. In the year 2018 I published the code under a free license on github.

With the current version 0.6 of the add-on, the monster script that I started with version 0.0.1 has become a bit more user friendly.

- A GUI based menu-system that even a Tails beginner or Linux novice can handle.
- Better integrated into Tails than ever before.
- Build a local socks5 server and make SSH connection to a foreign host over the Onion-Network. This cheap little trick allows us to visit tor-unfriendly websites inside Tails.
- Easy backup and restore of a complete persistent volume of a Tails USB stick.
- Can be upgraded over git on the fly ...

Have fun with my little add-on to enhance your user experience with Tails.

Best regards
swtor00

1. Introduction

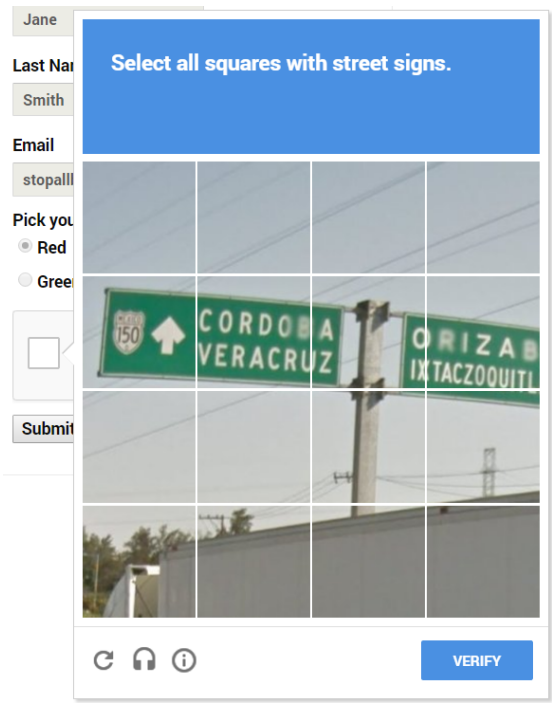
This documentation describes how to install and use this add-on for Tails-Linux. You may ask yourself, why do I need such a add-on for Tails ? The Tails Linux system already protects your privacy by using the Onion-Network on every startup in the background. It is also true that a Tails system already makes a very good job to hide your true identity and the real WAN IP-Address to the websites you are visiting. To be honest, this job is much better done by the people behind the Tails OS and their supporters that anyone else could do it alone by installing the TOR-Browser bundle on a regular Windows-Computer or a Linux-System. If I would be ironic, the only real purpose for TOR-Browser for Windows is to downloading Tails.

Although, it seems many Tor-Browser and Tails-Linux users are having difficulties surfing and navigating the regular World Wide Web (sometimes also called the Clearnet Internet) , as some websites have set up discriminating rules against people who are using the Tor Browser to browse the web. At any specific moment in time when we are using Tails or the Tor-Browser in general, our personal IP packets are sent through the Internet crossing 3 different Nodes to hide the origin where the packets came from.

The so called “Exit-Nodes” of the Onion-Network can easily and instantly be detected as soon as someone queries with any remote IP Address from the URL below.

https://check.torproject.org/torbulkexitlist?ip=1.1.1.1

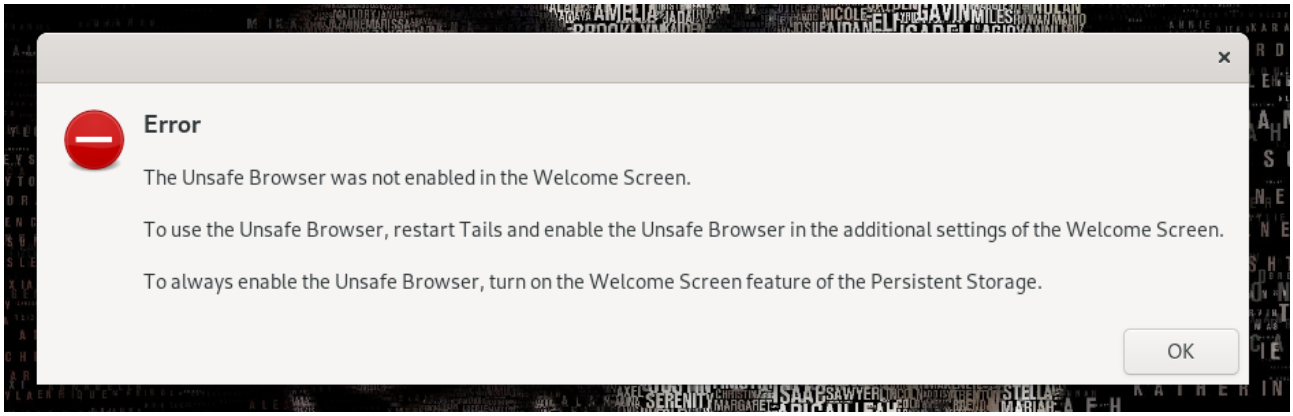
Therefore it is no longer a hidden secret to any visited website, that we are using the TOR-Browser or even Tails and they will often run this act of brainless “captcha terror” against regular users of the Tor-Browser. Right after here, you see a example of this so called “captcha terror”.



Alarmingly, the number of websites that even completely block or run the “captcha terror” against regular Tor users is growing in numbers day by day, to the detriment of Tor’s usefulness.

Integrated inside of every Tails installation on a CD or USB medium, there is still the so called “Unsafe Browser”. Because this “Unsafe Browser” doesn’t make any use of the Onion-Network that Tails provide in the background, all data communications from this “Unsafe Browser” can easily be logged by your internet service provider (ISP) or your government or any Network Administrator from a Hotel. After Tails version 4.8 was released,it was not longer possible to start the “Unsafe Browser” inside of Tails.

After Tails Version 4.8 was released, you see the following window on your screen by starting the “Unsafe Browser”.



With the default settings from the welcome screen of Tails 4.8 or higher, the start of the “Unsafe Browser” is not longer possible until a user set the default value from “not starting “ to “allow starting” inside the welcome-screen of Tails.

It may only make sense to use the “Unsafe Browser” inside Tails solely to browse a captive portal like it is used in many public WiFi networks or hotels for connecting, but not really for more than this simple task. In next URL you may find some other useful Information about “Unsafe-Browser”

https://tails.boum.org/contribute/design/Unsafe_Browser/

Prior to activating the use of the “Unsafe Browser” in the welcome-screen of Tails, please keep the following in mind.

- IF YOU DON’T NEED THE UNSAFE BROWSER OF TAILS ...PLEASE DO NOT ACTIVATE IT IN THE WELCOME-SCREEN OF TAILS AND NEVER USE IT UNDER ANY POSSIBLE CIRCUMSTANCES !!!!

- AT THE SAME TIME YOU ARE USING THE UNSAFE-BROWSER OF TAILS AND VISITING A EXTERNAL WEBSITE ANYWHERE ON THE INTERNET→ YOUR REAL IP OF YOUR CURRENT USED WAN INTERFACE WILL BE LEAKED IMMEDIATELY TO THE REMOTE SITE !

Some smart people even try to start a VPN connection with OpenVPN or something similar to hide the fact that they are using the Onion-Network ,which can be blocked by any website or even an ISP.

Apart from the fact that you are only able to use a single TCP port for a VPN communication (all UDP ports including ICMP Messages inside of Tails are blocked by default), it produces many more problems than it would solve.

In the endless debate in multiple forums on the Internet about the use of a Virtual Private Network (VPN) inside of Tails, I recommend to read the following URL completely.

https://tails.boum.org/blueprint/vpn_support/

The developers of Tails (and they know Tails from the ground up with every little detail that other so called technical experts don't even know yet) have a loud and clear statement to integrate any kind of a software like OpenVPN into Tails Operating System.

- NO NO NO and a big NO again !

The only clean and acceptable way for the multiples of developers of Tails to have a fixed outgoing IP address (that is not part of the Onion-Network of course) is to create a local socks5 Server and to build a SSH-Connection to a remote Host.

Now, exactly right here, my special add-on for Tails enters the game called "Enhancing Tails with a kind of VPN," and provides some very useful functions for the many Tails users out there.

- Use of an encrypted SSH-connection to a remote host and building of a local socks5 proxy. Even the traffic that is sent over the so called "Exit-node" of our communication is still encrypted until it reaches the destination SSH-Server. When the connection packets leave the SSH-Server to any external website for example, the packets are not longer protected by SSH itself and would look like any normal network traffic from a standard Desktop computer running with Linux.

- All SSH traffic is encrypted and routed over the Onion-network, as long you are using an SSH server anywhere on the Internet. If you are using a SSH Server in your own network at home, only the connection from your Tails system to the internal SSH server is encrypted. And I assume that this is not the way you would like to go about hiding the fact that you are using Tails.

- A local Browser (Chromium) with three different profiles that can be used to visit TOR unfriendly websites like youtube.com and many others that would block regular TOR users like second class internet users. All three Chromium profiles are protected against multiple actions like Web RTC and multiple other trackers in general.

- All local DNS resolution traffic on UDP Port 53 for Chromium is routed over the local socks5 proxy to the remote SSH server . This means you never contact your local DNS server from your currently used network or ISP, like you would do with the activated "Unsafe Browser" of Tails. And I say it again, just as a very important reminder.
  Do not activate the "Unsafe Browser" !

- For any particular website that we are visiting with Chromium on the Internet, it is no longer possible to detect that we are using the so called “Onion-Network” to hide our personal information, or even more important our current public IP-address at all. All the traffic that the owner of the website can analyze, is coming from the regular public IP address of the remote SSH server we are currently connected to.

One real huge problem still remains with using the Tails system to contact onion-unfriendly systems at all. It makes no difference what kind of working bypass protocol we are using to hide the fact that we are using Tails in the background. These so called bypass systems could be done by one of the following 3 techniques.

- Possible Bypass System 1 (Using SSH to build a local socks5 Proxy)

This is the way this add-on works and is the preferred method by developers of Tails. The add-on itself only use already installed Tails software to create our secured SSH connection.

- Possible Bypass System 2 (OpenVPN Server with a single TCP port)

OpenVPN is a very popular software for creating any kind of VPN. Most of all public OpenVPN servers on the Internet (there are multiple thousands of them on the net) only work with a single UDP port to connect. The UDP protocol is multiple times faster than the TCP protocol. This is one of the main reasons, why so many OpenVPN servers only providing UDP ports for connecting. There are not so many OpenVPN servers out there on the Internet, that can be used with the TCP protocol. Please take a closer look at the OpenVPN Servers on the following URL and you see what I mean. Almost 98 % of all servers only provide UDP ports for connecting.

https://www.vpngate.net/en/

This very accurate list shows multiple free OpenVPN Servers worldwide. I use this impressive list of free OpenVPN servers very often to watch live TV and read some newspapers from my current location while I’m on vacation, because every connection attempt from a foreign Country is blocked inside my own Country where I live. I use this list very often with a OpenVPN client under Linux or even Windows. But not within Tails, for a few several understandable reasons.

It is one thing to only watch a harmless TV show over a public VPN server that is managed by a person that I don’t know in person and log all my connections over this server, but it is a completely different kind of story to send any kind of sensitive data to a server that can be trusted for 100 %.

- Possible Bypass System 3 (proxychains)

With my first experiments with Tails to establish a stable connection to a few TOR unfriendly websites I was using this tool called proxychains. Sometimes it worked for me more or less not too bad but a half hour later the program stopped working without any clear reason to me. In my humble opinion it wasn't the right tool to do the job properly. You may test it for yourself, you may come to a different conclusion than me.

https://shorturl.at/eyF89

The following 3 very often used VPN protocols don’t work inside Tails.

- LL2TP
- IPSec
- WireGuard

All of the above listed well known protocols are using or are depending of one or multiple UDP Ports to work properly. Inside Tails it isn’t possible to create a simple UDP connection directly to the Internet.

A big Warning about using any of the 3 working presented bypass techniques including the remote ssh-servers that you are using with my own add-on here:

At this point I would like to raise awareness about the trust you are willing to give to a foreign host system and his administrators or users, which could easily read your complete communication that would be sent through to the foreign server over Tails. If you would like to use any of the 3 working bypass techniques, please don’t underestimate the control they have over you in the exact moment in time that you are using their servers.

Almost any VPN or SSH Service provider worldwide out there on the Internet make claims on their websites with really cheap marketing statements like the following ones:

“We don’t log anything !”
“We don’t spy our users !”
“We protect the privacy of our customers !”

To be honest. That’s in the most cases only cheap marketing crap for foolish customers, that truly believe that marketing bullshit published by the company who offers the Service. Some very interesting articles about the so called “no-log policy” of some important worldwide VPN providers can be found right here.

https://shorturl.at/ijmzE

https://shorturl.at/csRT7

https://shorturl.at/eBTV3

If you read the above articles carefully, you may come to the final conclusion that you shouldn’t give your personal trust out to the first person or company who offers you a VPN or a full SSH account for free. Even if you pay for a service with a monthly fee, there is no guarantee that you aren’t being “tracked” by this VPN server or any other active users of the remote system. Some very insane and shameless VPN providers do make a second business with selling the collected VPN data to other company's for marketing purposes.

If we are talking about the trust you are willing to give to a company or a remote server, we should also talk about one of the securest email providers out there on the Internet called Proton-Mail that reside in Geneva / Switzerland.

The company Proton also claims that no log files are generated. The french customer of Proton mail who was arrested 2021 by the police, may see it completely different. He was using his free Proton mail account over the normal URL of the Clearnet Internet instead over the onion address that Proton provides for the customers. If this french customer of Proton had used the TOR-Browser to access his mail, he would still be free.

https://account.protonmail.com/login

This was the URL he had used prior he was arrested.

Proton gave the french police department the public WAN IP-Address he was using to get his personal mail. A few hours later he was arrested by police and wearing handcuffs. Be reminded again, when a company says to the public what they would never do ...
they'll do it for sure, if they have to !

https://shorturl.at/nFJRW

If you are using Proton mail (I do it as well → swtor00@protonmail.com), my personal advice is clear. Only use the onion V3 address of Proton. Even for registering a new account.
Only use the new onion V3 address to check your Email.

https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/login

This means you should do this only with Tails ! .. and DON'T under any circumstances check your private Proton mail-account with a standard PC Operating System like Windows outside of Tails.

Prior to showing 3 possible working SSH scenarios with the add-on, we have to talk about the dangers of using it at all. From all the described SSH scenarios in the next chapter, you should only use the last presented scenario whenever possible.

- Never create a login with a username / email-address/ password that you have ever used on the standard internet at anytime.

  A special note about the above rule, if you are living in a country like China or something similar that completly blocks Gmail. For example, if you are the owner of a Gmail account, you would never have a real change to login over the TOR-Browser. With the help of the add-on, it would be possible to get a chance to Login for that particular Gmail account. That's the only possible exception !!!
  If you don't need any access to a Gmail account. Stay away from using Google.

- If you need a valid Email-Address to register for a service or something similar, while you are using Tails, you have to create a single Email-Address that you would only use inside of Tails and nowhere else.

  NEVER TRY TO ACCESS OR PUBLISH THIS SPECIALLY CREATED EMAIL-LOGIN TO ANYONE OUTSIDE OF TAILS !!!!!!!!

  NEVER SEND AN EMAIL FROM YOUR ORDINARY EMAIL TO THIS TAILS ONLY GENERATED EMAIL ADDRESS !!!!

  NEVER SEND AN EMAIL FROM THE TAILS ONLY EMAIL TO ANYONE THAT YOU EVER CONTACTED BY YOUR ORDINARY EMAIL SYSTEM AT HOME OR IN A BUSINESS !!!

- These kind of digital fingerprints (Emails / nicknames / passwords and many more little things that you often not think about) could be easily tracked back to you as a person with enough effort and time.

- Only use the add-on to solve problems with tor-unfriendly sites at all and if possible use every time the more secure builtin TOR-Browser of Tails to connecting it.

- You should never use a personal credit card to pay anything, that points directly to you.

- You never use any kind of 2 factor authorization that needs a mobile number to register.

- Never use any websites simultaneously inside the TOR-Browser and the Chromium Browser used by the script. This is because in case your internet is going down, both of your connections will terminate at the same time, and it will not be hard for someone spying on you to recover the pieces and complete the puzzle. It may be better to use only one browser at any one time and not trying to mix them up.

- We are already in the year 2021 and we still have millions of dummy websites that still use these stupid old fashioned http:// instead of the secure alternative https://.
  You very well know that TOR can be exploited using the vulnerabilities present at its exit nodes. So, if you access HTTP sites using TOR, there are chances someone might access your information while it is on the endpoints. The data transferred to and from an HTTP site is not encrypted and can be viewed at the endpoints as TOR only encrypts the connection inside its own network. You can prevent such situations by the use of HTTPS websites. They use end-to-end encryption protocols like SSL (Secure Socket Layer) and TLS (Transport Layer Security). So, all your data remains safe, even if it is outside the TOR network to the final destination.

- Never wait more than a few days to update the Tails system if possible. It is very important that you always use the latest stable release of Tails.

- Only use search engines inside browsers that do not store personal settings in any kind. There are 2 known public search engines that do this, they don't store anything about your searches, and so far to date 2021 these two search engines haven't been caught doing this.

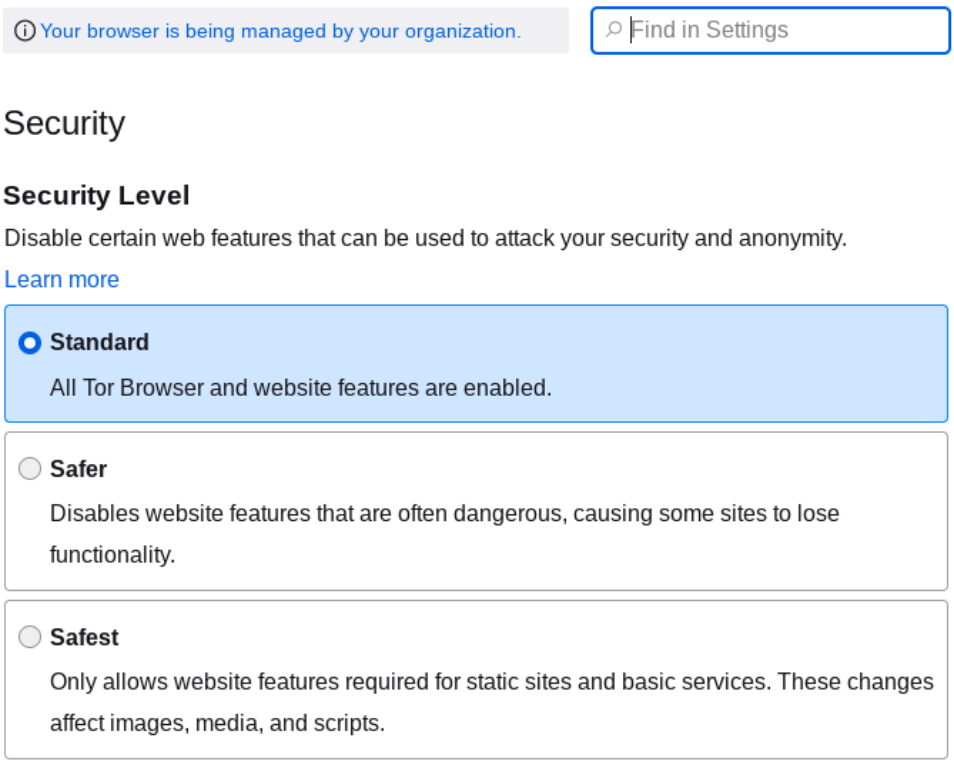
  https://www.startpage.com

  https://duckduckgo.com/

- Do not use and activate the unsafe Browser of Tails. Yes, I know this is the third Warning I gave ..

- Do not try to install any P2P software like Torrent or something similar.

- Some people suggesting a increased security-Level for the TOR-Browser that can be set by the user anytime.



Be warned by me : If you increase the Level to the mode "Safest", almost any modern Website is looking horrible uggly and is more or less useless. I did never increased this Level during the long time I was using Tails.

- If you are downloading any kind of files with any of the 2 Browsers inside Tails (like any Microsoft Office Files as a simple example) , please don’t try to copy them to USB and open them in a other Operating System like Windows with an installed Office in place. What you are downloading with Tails should only be opened inside Tails and never leave Tails. What happens in Tails → remains in Tails.

  You may read carefully the following URL and you should never open any Excel sheet outside of Tails , that you have downloaded with the TOR-Browser of Tails.

  https://shorturl.at/mpwO0

- Do not try to install the TOR-Browser Bundle on an ordinary Operating System like Windows and use the same credentials you created already for Tails only. If you really have to go this highly not recommended way, then you have to create new emails and SSH accounts for every system.

- Save the data from the persistent volume of Tails on at regular intervals. This backup should be placed on a very secure location inside your own residence or even better transfer the backup with SSH to a remote host in another country than your current one. And yes, with SSH you can copy files to a remote host as well. And when you need this backup, in case of a damaged stick (some call it a Tails emergency) , you need the following information to copy back the backup to a new Tails stick.

  - DNS name or IP address of the backup server
  - Port for connecting
  - username and password
  - Exact location of the backup inside the user-directory
  - You may also need the SSH-keys if you can not login with a password

  It would be very good practice to try out this “emergency-scenario” as long as you still have a working Tails. If you have a real “emergency” it could be too late to copy the image back to a new Tails.

- Use a strong and long password for the persistent volume of Tails.

- Always try to shutdown the Tails-OS the clean way.

- If you are using Tails in public areas like a library or a restaurant, never simply walk away from the Computer running Tails with the unlocked persistent volume. The first action should be to “Lock” the running Tails. After you have “Locked” Tails , you can safely walk away.

- Never try to visit any Tails or TOR related Websites with a normal browser using a Windows or Linux System. This following websites especially.

  https://tails.boum.org/
  https://www.torproject.org/
  https://gitlab.tails.boum.org/tails
  https://www.reddit.com/r/tails/

  You know, what the funny thing is about the subreddit for Tails on reddit.com ?

  There are a lot of active Tails users on that forum that try to be as “Anomymous” as possible as long they are using Tails and the first thing they do is the following ... one from reddit as a example ! They register for a new reddit account with a private or even worst with a business email-address for posting on that forum. Of course all done with an ordinary browser with a Windows or Linux OS.

  Or maybe this one .... as a last very ironic example from me, how you shouldn't post a photo on reddit :

  You have a strange error message inside of Tails and you don’t know what do with this message ? You take a photo of the error-message with your smartphone and post this photo directly to the Tails forum on reddit ..… There are so many nice users of Tails in that forum, someone may know the solution to your problem right ? You are probably not aware of this, but the following worst case scenario can happen very quickly.

  - The serial and IMEI number of your smartphone are hidden in the Meta- Data of the photo that you made with your phone.
  - The exact location measured with GPS may also be included in the Meta-Data.
  - And last but not least , the same photo may also already be stored in a Google or Apple cloud depending on the OS by the used Smartphone.

Please do not underestimate the amount of Information that could be hidden inside the Meta-Data of the following file types (only a few example).

- Photos with multiple information like described above.
- Generated PDF’s that contain the serial-number or the Adobe Live-ID of the product used to produce this PDF.
- Office documents may contain a serial-numbers/company name or even a offical Microsoft Live ID if you created the document with a Office 365 Account on a other computer.

Below you’ll find a very good overview with multiple examples about the real danger of Metadata inside photos and PDF files or word documents :

- https://shorturl.at/ityS5

Inside previous releases of Tails was a little tool preinstalled called MAT to remove unwanted META data from multiple types of files. Since Tails 4.23 this handy tool is no longer part of the system. If you need to remove MetaData from a file within Tails 4.23 or higher, you should install the software within a root terminal.

---

apt-get install mat2

The bad news for some not so experienced Tails users may be a little shock. This new mat2 application doesn’t have a nice GUI Interface. It works only on the command line of Tails (Terminal). We hope the developers of Tails do make a GUI replacement soon.

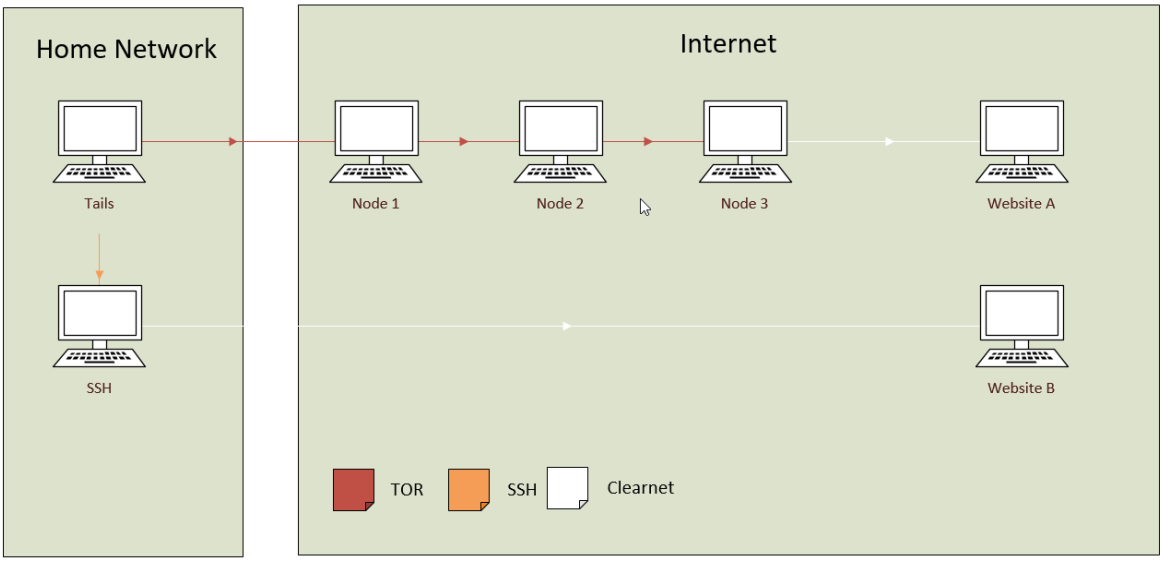
You may find all of my above security tips for using Tails in a secure way are way to ridiculous or excessive, but if you are living in a Big Brother Country like China with a very strong Internet censorship these tips and tricks may help you to stay free instead of being recognized and identified as a Tails user with all the possible consequences.

1.0 Using your own SSH server inside your own Network at home

For this simple and not really recommend scenario, you need at minimum, a second computer with Linux or Unix running on your own network at home. For this SSH-daemon you could use, for example, a simple Raspberry-Pi, or of course, any other computer with an SSH daemon would work as well. This could be implemented with a Linux System like Debian or many others without any problem. For a simple example to build a standalone SSH-server on a Raspberry-Pi I would recommend the following URL.

https://shorturl.at/lsEQT

Scenario 01



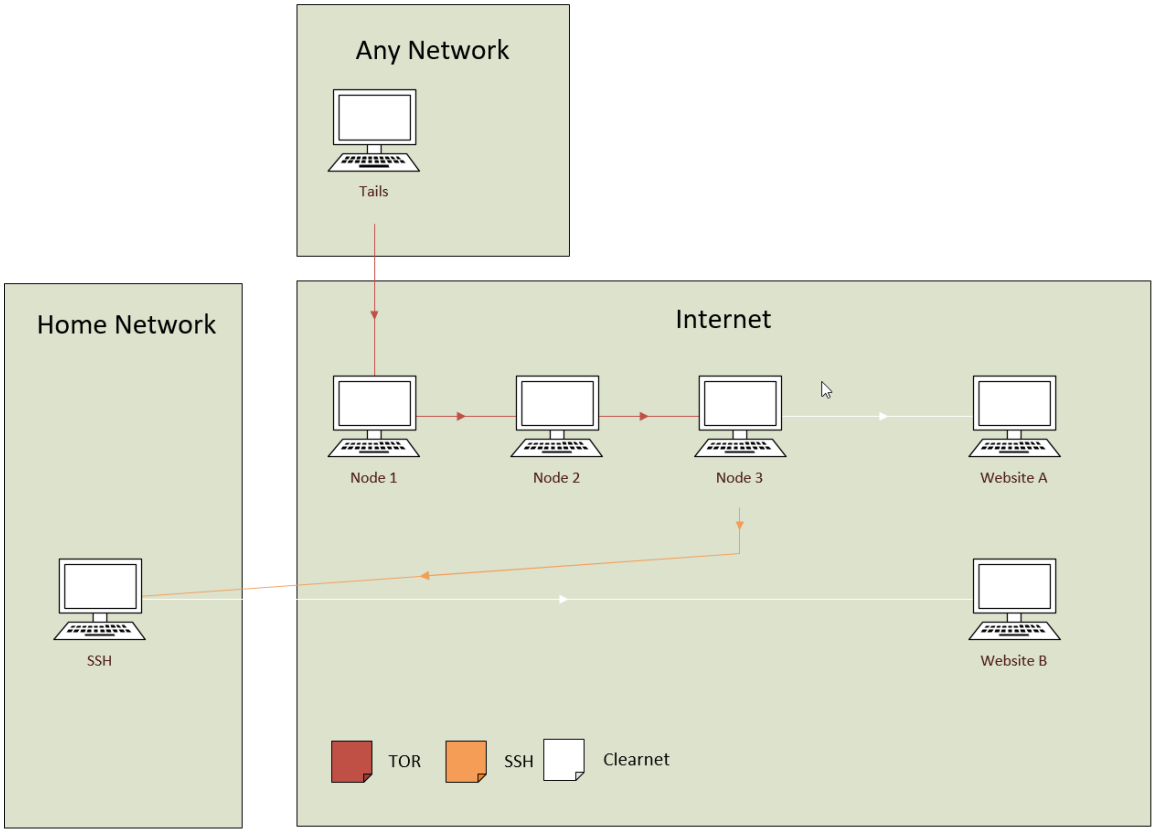
If you are using this “not so perfect first scenario 01”, you can do the following:

- Use a Website like Google or many others that normally would block your connection as soon you are trying to use it inside of Tails. To be reminded again ! The complete Internet traffic (Data) that you send via my script through the Internet (from the SSH-server at your home to Website B for example → the white line in the graphic), can be tracked and analyzed by your current ISP, because it would be coming from a regular computer inside your own home network ! Only the websites that you are visiting with the TOR Browser over the Onion-network are secure to visit without to being tracked (Website A for example → the red line in the graphic). After the data is encrypted in the last node, the data leaving the exit-node of the onion-network, the network traffic is now showing again in the white color.

- Because the destination SSH-Server is inside the same physical network, the data you are sending from tails to this server aren’t crossing the router into the direction Internet. These packets aren’t routed over the 3 external nodes, because this network traffic is only local.

2.0 Using your own SSH-server that can be used when you are not at home

Scenario 02 :



If you would like to connect to the home ssh server externally from the Internet with Tails, there is some additional work to do.

- Port Forwarding of TCP port 22 (or any other desired port you would like to use) to the destination IP inside the home network needs to be enabled. This has to be done inside your router or firewall, depending what device you are using to connect to the Internet. Most users own a router for connecting to the Internet. Please consult your router manual for the correct implementation of Port Forwarding for your device.

- In the same moment you are making the internal ssh-server reachable over the internet by Port Forwarding, there are some very important settings for the ssh-server that should be done prior to install and activate Port Forwarding on your router. All the recommended security settings for the ssh-daemon are stored in the file sshd_config.

- Do not allow root Logins over SSH (PermitRootLogin no)

- Allow only a single user to login over SSH (AllowUsers freaky)
  In the above example only the user “freaky” could make a ssh-connection to the ssh-server.

- You may not use the standard TCP port 22. A very good replacement port would be TCP port 443 or 53.

  Port 443
  Port 22

  In the above sample setting for sshd_config , the server would listen on port 22 and 443 for incomming ssh-connections.

- Only allow a ssh login with a key instead of a password. As long you don’t have a user-key use this configuration inside sshd_config.

  PubkeyAuthentication yes
  PasswordAuthentication yes

  As soon, you can login with a key change the value to:

  PasswordAuthentication no

  Or would you like to have not so nice intruders on your ssh-server from China and Russia that are trying to guess your root password the hole day ? This is specially true if you are using the standard port 22 for SSH.

- Only use SSH-V2, The older protocol V1 shouldn’t be used anymore.

  Protocol 2

- Fake the login message to mislead the snoopers or any disliked person.

- Put the SSH-daemon on a schedule, if you know you’ll want it before hand.

- Always update your system to the latest versions available because your computer could be contacted directly from the Internet.

- Your computer at home needs to be up and running all the time. if you want to contact the your home server from any location via the Internet.

- Enable a DYNDNS name for your WAN IP, because most ISP‘s don’t provide fixed IP-Addresses for the customers WAN interface. If you need a DYDNS name for your connections to the home network, I would call it a security hole that your often not aware of. On of the best and securest DYNDNS provider you find here.

  https://shorturl.at/gDQZ8

I would like to emphasize the importance of the fact, like in the previous scenario 01, all traffic that you send out over my script can be traced by your home ISP or a local government. If you are placing a server like this in a company environment, the staff of the involved company could also be tracking all your traffic that you are sending over tails with my script. This is of course only true for the traffic that leaves the SSH-Server into the direction of the Internet.